NB Refer to lecture handouts for diagrams for DES and Needham - Schroeder.

E4.44 Network Security Specimen Exam Paper 1

Answer 4 questions

Time allowed: 3 hours

1. (i) Fig 1.1 shows the round structure for DES encryption. Explain how decryption can be achieved with this structure.

   (ii) Fig 1.2 shows how the per round keys are generated in DES. What is meant by weak keys and identify the four such weak keys. What impact does use of a weak key have on DES

   (iii) What is meant by an exhaustive key search? How many keys should be investigated to find a particular key used in DES?

   (iv) Explain how the security of DES may be increased by the use of 3DES. By how much does 3DES improve the strength of DES?

   (v) In the IDEA algorithm addition is performed modulo 2^{16} and multiplication is performed mod $2^{16}+1$. Given that these operations transform a 16-bit message segment into another 16-bit message segment though the application of a 16-bit key explain how these operations can be reversed.
   In order to create a new algorithm with the same structure as IDEA but with simpler operations using 8-bit numbers it is proposed to perform addition modulo 2^8 and multiplication modulo 2^8+1 . Discuss whether these operations would be reversible.

2. (i) Show that for two prime numbers p and q and n = p.q, ϕ(n) = (p-1).(q-1).

   (ii) In RSA explain why the message to be encrypted must be smaller than the public key modulus n. A small message less than a third of the length of the public key modulus n (in binary form) is encrypted in RSA using a public key exponent of 3. How can the ciphertext be deciphered without the use of the private key?

   (iii)Explain how the Diffie-Hellman key exchange can be used to establish a session key in secret key cryptography. Explain why a passive observer would be unable to establish the session key despite observing all communications.

   (iv) How can a bucket brigade attack be launched against a Diffie-hellman key exchange? Discuss one way in which protection against such an attack can be provided.

3 (i)You are provided with the following:

- an RSA facility complete with public/private key pair
- a CBC facility incorporating the IDEA block cipher
- a message digest facility employing the MD5 algorithm.

You are required to send a block of data of size 1 Mbyte through an insecure network to a recipient who knows the message digest you are using, your secret key in IDEA and your RSA public key. Explain how you would use your security facilities (each facility for one operation) to provide the security services of privacy, message integrity and source authentication.

(ii) How would you achieve the above if the RSA facility were not available? Discuss the relative security strengths of your solutions to (i) and (ii).

(iii) In order to reduce the computing power required for MD5 it is proposed to devise a new message digest function in which the message is first divided into 64-bit blocks. The odd numbered blocks (first, third, fifth etc) are added together modulo 2^{64} to provide the high order half of a 128-bit message digest. The even numbered blocks are added together in a similar fashion to form the low order half of the message digest. Discuss the security implications of using this message digest in your designs for (i) and (ii) above.

4 (i) Explain the terms "proof of submission" and "non-redudiation" in an electronic mail system. Explain the importance of non-repudiation in a system if e-commerce.

(ii) An attacker is intent on disrupting secure communications by inserting bogus packets (with correct TCP checksum) into the communications. Discuss how such an attack would succeed in systems protected by IPSec and SSL.

(iii) What is meant by "Endpoint Identifier Hiding"? Explain one method by which it may be provided.

(iv) What is meant by "Perfect Forward Secrecy"? Does Kerberos offer Perfect Forward Secrecy?

5. (i) What functions should be provided by a public key infrastructure? Is it possible to operate a public key security system without a public key infrastructure?

(ii) Discuss the following models of public key infrastructure citing practical examples which follow the model.

(a) anarchy

(b) oligarchy
(c) policy based certificate hierarchy

(iii) A particular PKI issues Certificate Revocation Lists whenever the number of revocations made since the last list was issued exceeds a pre-set figure. Discuss how such a system could be attacked.

6. (i) Figure 6.1 shows the Needham- Schroeder system of authentication. Explain the purpose of each of the five messages in the interaction. What are the functions of the numbers N_1, N_2, and N_3 ?

(ii) In Kerberos V4 a client and its server are connected to different KDCs. Explain the process by which the client authenticates itself to the server.

(iii) Explain how the process in (ii) differs in Kerberos V5. What are the other differences between Kerberos versions 4 and 5?